What is claimed is:

1. An integrated computer emergency response system comprising:

an information collecting/managing section for collecting security information about a wide range of security incidents and vulnerabilities which may be a threat to systems to be protected, via nationwide or enterprise-wide information technology infrastructures, including computer systems or networks, applications and internet services, and storing source data;

an information processing/analyzing section for processing and analyzing collected security information using a predetermined analysis algorithm and storing and managing analysis results;

an operating system section including an information sharing/searching/announce unit for transferring the processed and analyzed information to at least one system to be protected or an external system and a display unit for outputting necessary security information in a predetermined form;

an information security section for protecting the integrated computer emergency response system's own information; and

a database section including a vulnerability DB for storing vulnerability information and a source/processed DB for storing source data and processed data.

2. The integrated computer emergency response system according to claim 1, further comprising an CERT/ISAC/ESM to CERT/ISAC/ESM interworking section for interworking with external systems, including ISACs, CERTs and ESMs, in order to share reliable information.

3. The integrated computer emergency response system according to claim 1, wherein said information collecting/managing section includes a vulnerability DB collecting unit for collecting, classifying and processing vulnerabilities officially recognized and provided by various domestic or foreign company system hardware vendors and OS (operating system) vendors.

4. The integrated computer emergency response system according to claim 1, wherein said information collecting/managing section includes a vulnerability scanning result collecting unit for periodically scanning vulnerabilities and collecting scanning results.

5. The integrated computer emergency response system according to claim 1, wherein said information collecting/managing section includes an information security data collecting unit for collecting and storing information

security data or references published by CERTs or ISACs, colleges, research centers and government companies with respect to security incidents, including hackings, and countermeasure against the incidents, using an automated collecting tool, such as a web robot or a search engine.

6. The integrated computer emergency response system according to claim 1, wherein said information collecting/managing section includes a virus/worm information collecting unit for collecting and storing information about computer viruses or worms using an automated collecting tool, such as a virus alert system, an agent or a search engine.

7. The integrated computer emergency response system according to claim 1, wherein said information collecting/managing section includes an incident report collecting unit for receiving security incident reports through communication means, such as telephone, facsimile, e-mail and web sites, and storing information about reported incidents.

8. The integrated computer emergency response system according to claim 1, wherein said information collecting/managing section includes a system asset information collecting unit for collecting and normalizing

information about systems and network devices involved in the integrated computer emergency response system and asset information relating to the significance (asset values) of the systems and the network devices and storing the collected information.

9. The integrated computer emergency response system according to claim 1, wherein said information collecting/managing section includes an event collecting unit for collecting and storing in real time events relating to information security from at least one information security product of a firewall (F/W) system, an intrusion detection system (IDS), a policy management system, a anti-virus product, a PC information security system, a retracing system, a PKI certification system, a network device and a virtual private network (VPN).

10. The integrated computer emergency response system according to claim 1, wherein said information processing/analyzing section includes:

a dataware housing unit for normalizing information collected by the information collecting/managing section in various categories and establishing a database storing information; and

an information analyzing unit for analyzing the information stored in the database established by the dataware housing section by applying a data mining or knowledge-based analysis algorithm and an analysis algorithm for analyzing security incidents and vulnerabilities, correlations with major assets, recognizable patterns and classifications for preventing incidents and vulnerabilities.

11. The integrated computer emergency response system according to claim 10, wherein said dataware housing unit receives security data, classifies the received information, determines whether the data need be summarized or processed, and if required, summarizes the data according to search types or adds a data field to generate a database.

12. The integrated computer emergency response system according to claim 1, wherein said information sharing/searching/announce section has a profile management function of classifying information to be shared according to types or classes and users/companies who will share information according to classes and a information providing function for receiving a user's request for information search and providing the requested information to the user's system.

13. The integrated computer emergency response system according to claim 2, further comprising an attack assessment section for performing attack assessments for

security incidents, such as hackings or cyber terror, classifying the incidents based on past attack methods and frequencies, supplying possible attack scenarios and automatically implementing attack assessment functions, including databasing of vulnerability analysis results, real-time analysis of critical attacks, collection and analysis of important packets and issuance and spread of a forecast/warning, in a pre-defined manner.

14. The integrated computer emergency response system according to claim 13, further comprising a test-bed for supplying a possible scenario when a new security incident or vulnerability is detected and performing a simulation under the same condition of a system to be protected so that an attack level and any damage and effective response can be expected.

15. The integrated computer emergency response system according to claim 14, further comprising an early forecast/warning section for generating an alert signal to the results issued by the test-bed or attack assessment section and sending the alert signal to a system to be protected or an external system to inform of any security incident or vulnerability.

16. The integrated computer emergency response

system according to claim 2, further comprising an asset evaluation/recovery period calculation section for evaluating the significance or asset value of a system to be protected and anticipating damage resulting from a possible security incident and a recovery period based on the evaluated significance of the system.

17. The integrated computer emergency response system according to claim 14, further comprising an automatic education/training section for generating educational information from the results of a simulation performed at the test-bed, storing and managing the educational information and sending the educational information to an external terminal that requires education.

18. The integrated computer emergency response system according to claim 1, wherein said information security section for protecting the integrated computer emergency response system's own information includes:

a physical information security unit including at least one of a card certification unit, a password certification unit, a biometrics unit and a CCTV; and

a network/system/document security unit including at least one of a PKI certification system, an intrusion detection system, an anti-virus system, a retracing system and a watermarking system.

19. The integrated computer emergency response system according to claim 2, wherein said CERT/ISAC/ESM to CERT/ISAC/ESM interworking section includes:

an information management unit for processing, analyzing and taking statistics on information to be exchanged with external systems in an encrypted standard format and classifying companies according to user classes; and

an interface for performing an access control (providing data according to user classes) and a protocol conversion for data exchange with external systems.

20. The integrated computer emergency response system according to claim 3, wherein said database section includes at least one of:

a vulnerability DB for storing a list of various vulnerabilities of relevant systems and a vulnerability checking list;

a source/processed DB for storing source data and processed data of collected security information;

a reported incident DB for storing incident information inputted through the incident report collecting section;

a blacklist DB for selecting habitually occurring incidents from the list of vulnerabilities and security incidents and storing the habitual incidents;

an alert DB for selecting incidents about which an early forecast or alert is required from the list of vulnerabilities and security incidents and storing the selected incidents;

a profile DB for storing information about relevant systems and users; and

an incident history DB for storing previous incidents and vulnerabilities, together with countermeasure against such incidents and vulnerabilities and various log files.

21. The integrated computer emergency response system according to claim 3 or 20, wherein said database section includes a computer forensic DB for extracting information about events recognized as computer crimes from records of attacker IP addresses which were or can be origins of critical attacks and storing the extracted information for use as evidence later when a victim of a security attack files a criminal complaint or a civil action, seeking compensation for any financial damages or losses.

22. A method for responding to a security incident by using an integrated computer emergency response system, which comprises:

an information collecting step performed by an information collecting/managing section to collect security information about security incidents and vulnerabilities through a predetermined communication network;

an information processing/analyzing step performed by an information processing/analyzing section to database collected security information and analyze the databased information using a predetermined analysis algorithm;

an information sharing/searching/announce step of managing processed and analyzed security information to be shared and searching for and providing the information upon request; and

an alerting step of sending predetermined early warning information to at least one of any inside and outside systems if an alert is required for any incident or vulnerability.

23. The method according to claim 22, further comprising a step of automatically protecting the integrated computer emergency response system's own information by using a predetermined information security section.

24. The method according to claim 22, further comprising a step of managing information which was generated by the integrated computer emergency response system and may be shared with other companies, and transmitting the information to systems of other companies that require such information.

25. The method according to claim 22, further comprising an attack assessment step of automatically assessing the attack level of each security incident or vulnerability using the attack assessment section and determining any need to issue an alert or establish a computer forensic DB or a blacklist DB according to the assessment results.

26. The method according to claim 22, further comprising a test (simulation) step of performing a simulation of a new security incident or vulnerability under the same condition of a system to be protected and storing simulation results.

27. The method according to claim 22, further comprising an asset evaluation/recovery period calculation step of evaluating the asset value of a system to be protected based on a pre-inputted guideline and automatically calculating at least one of a recovery period and damage when a security incident occurs.